REMARKS

In the Final Office Action, Claims 1-36 were examined and are rejected. In response to the Office Action, Claims 1, 10-12, 21, 26-27, 31 and 34 are amended, no claims are cancelled, and no claims are added. Applicant respectfully requests reconsideration of pending Claims 1-36 in view of the following remarks.

I. Objection to the Claims

The Examiner has objected to Claim 27 for including an informality. In response, Claim 27 is amended in accordance with the Examiner's request. Accordingly, in view of Applicants' amendment to Claim 27, Applicants respectfully request that the Examiner reconsider and withdraw the objection to Claim 27.

II. Claims Rejected Under 35 U.S.C. §112

The Examiner has rejected Claims 10 and 12 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

Regarding Claims 10 and 12, Claims 10 and 12 are amended to overcome the deficiencies identified by the Examiner. Accordingly, in view of Applicants' amendments to Claims 10 and 12, Applicants respectfully submit that such claims, as amended, particularly point out and distinctly claim the subject matter, which Applicants regard as the invention. Therefore, in view of Applicants' amendment to Claims 10 and 12, Applicants respectfully request that the Examiner reconsider and withdraw the 35 U.S.C. §112, second paragraph, rejection of Claims 10 and 12.

III. Claims Rejected Under 35 U.S.C. §102

The Examiner has rejected Claims 1-36 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application No. 2003/0054918 to Willey ("Willey".) Applicant respectfully traverses this rejection.

Regarding Claims 1 and 11, Claims 1 and 11 are amended to recite the following claim features, which are neither taught nor suggested by Willey:

> authenticating, by the host device, the detected wireless device based on the requested audio authentication initialization information received from the detected wireless device and audio authentication initialization information stored by the host device for initial authentication of the detected wireless device. (Emphasis added.)

According to the Examiner, Willey teaches the above-recited feature of authenticating, prior to the above amendment with reference to paragraphs 8-53. (See pg. 4, ¶ 8 of the Office Action mailed September 28, 2006.) As taught by Willey:

> In another aspect of the invention, the invention provides a method for establishing a key between a first device and a second device, and includes the step of establishing a shared secret in the first device and in the second device. The method also includes the substeps of calculating an antispoof variable based at least in part upon the shared secret in the first device and in the second device, the antispoof variable being represented by a plurality of digits; indicating the digits of the antispoof variable form the first device to a user using a first stimulus; indicating the digits of the antispoof variable from the second device to the user using a second stimulus; verifying that the digits of the antispoof variable form the first device and the second device are the same; and establishing the key based upon the result of the verifying step. (Pp. 2, ¶ [0018].) (Emphasis added.)

As further disclosed by Willey:

> The handset 100 indicates to the user 500 that in order to complete the paring procedure that the user 500 should verify that the digit string that is audibly played by the handset 100 via speaker 140 and the digit string that is audibly played by the headset 300 are identical. (Pp. 5, ¶ [0049], lines 7-12.) (Emphasis added.)

Based on the cited passages above, the pairing procedures between first and second devices such as telephone handset 100 and headset 300, as shown in FIG. 5 of Willey, in conjunction with the flow chart of FIG. 5A, describe the generation of antispoof variable 36. The generation of antispoof variable 36 is designed to avoid man-in-the-middle attacks that are

incurred when implementing the paring procedures using techniques such as the Diffie-Helman protocol (see p. 1, ¶ 6.) In order to avoid such man-in-the-middle attacks, the generation of symmetric key 36 (the 3 antispoof variables) to insure that both devices have the same secret key, the antispoof variable is verified as follows:

> In step 5, the handset 100 informs the user 400 via the display 160 that in order to complete the pairing procedure the user 400 should verify that each digit that is about to be displayed by the display 160 is the same as the digit that is announced simultaneously via the speaker 140. (P. 4, ¶ 0042, lines 1-5.) (Emphasis added.)

In the embodiment described above, the user verifies that each digit that is displayed on display 160 is the same as the digit that is announced by speaker 140 of handset 100. In an alternative embodiment:

> The handset 100 indicates to the user 500 that in order to complete the pairing procedure that the user 500 should verify that the digit string that is audibly played by the handset 100 via speaker 140 and the digit string that is audibly played by the headset 300 are identical. (P. 5, ¶ 0049, lines 7-12.) (Emphasis added.)

Based on the cited passages above, the user is required to verify that the digits of the antispoof variable provided form handset 100 and speaker 300 are identical. As further disclosed by Willey:

> After the user 400 has given positive confirmation on both the headset 300 and the handset 100, then the devices 100 and 300 are fully authenticated. In the next step 7, the devices 100 and 300 securely establish the link key. For example, the devices 100, 300 can both derive a symmetric encryption key based upon to the elliptic curve Diffie-Hellman shared secret. A link key is created, and encrypted using the encryption key and send to the other device 300 which decrypts and stores it. The link key is to be used by the devices 100 and 300 for BLUETOOTH authentication and encryption. (P. 5, ¶ 0048, lines 1-11.) (Emphasis added.)

Based on the cited passage above, verification of the antispoof variable enables secure establishment of a link key which is used by devices 100 and 300 for BLUETOOTH authentication and encryption. (See supra.)

Conversely, amended Claims 1 and 11 recite that the host device authenticates the detected wireless device based on the requested audio authentication initialization information

received from the detected wireless device and audio authentication identification information stored by the host device for initial authentication of the detected wireless device.

As mandated by case law, "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2USPQ2d 1051, 1053 (Fed. Cir. 1987). ("Verdegaal Bros")

Here, for at least the reasons indicated above, Willey teaches a pairing procedure for establishing a key agreement between first and second wireless devices that requires a generation of an antispoof variable once the devices have exchanged public keys by sending a message to the respective device (see pp. 2-3, ¶ 0018 and p. 4, ¶ 0040, 0041.) As further taught by Willey, the antispoof variable is based on a one-way function of a shared secret between the two devices.

As shown in FIGS 5A-8, the user is required to verify that the digits of the antispoof variable 36 between the wireless devices match by comparing audio digits from a handset device to the displayed digits or audio digits from the corresponding device (see p. 4, ¶ 0042 and p. 5, ¶ 0049.) Once the user verifies that the antispoof variables calculated by both devices are identical, the devices may securely establish a link key that is used by the devices for BLUETOOTH authentication and encryption. As disclosed by Willey, the antispoof variable is generated to avoid man-in-the-middle attacks.

Conversely, as recited by amended Claims 1 and 11, a host device stores audio authentication initialization information for initial authentication of a detected wireless device. Accordingly, when the detected wireless device fails authentication according to a requested device identification information, the host device authenticates the detected wireless device based on audio authentication initialization information stored by the host device for initial authentication of the detected wireless device.

In contrast, Willey teaches that a user is required to perform such authentication by comparing displayed or audibly played digits of an antispoof variable between wireless devices that are being paired by a user. Accordingly, as recited by amended Claim 1 and 11, a host device authenticates a detected wireless device based on audio authentication initialization

information previously stored by the host device that corresponds to the detected wireless device. In other words, as recited by amended Claims 1 and 11, the host device authenticates the detected wireless device based on the requested audio authentication initialization information received form the detected wireless device and the audio authentication initialization information stored by the host device for initial authentication of the detected wireless device

Applicants respectfully submit that the playing or displaying of the digits of an antispoof variable to a user to verify that devices being paired by a user contain identical antispoof variables does not inherently or expressly disclose the authentication by a host device of a detected wireless device using audio authentication initialization information stored by the host device for initial authentication of the detected wireless device. Such information may be used to authenticate the wireless device based on the requested audio authentication initialization information received for the detected wireless device, as recited by amended Claims 1 and 11.

Consequently, Applicants respectfully submit that Applicants' amendment to Claims 1 and 11 prohibits the Examiner from establishing a prima facie case of anticipation of amended Claims 1 and 11 since Willey fails to either inherently or expressly disclose authentication by a host device of a detected wireless device based on the requested audio authentication initialization information received from the detected wireless device and audio authentication initialization information stored by the host device for initial authentication of the detected wireless device. Consequently, Willey cannot anticipate the recited features of amended Claims 1 and 11. Id.

Therefore, Applicants respectfully submit that amended Claims 1 and 11, as well as dependent Claims 2-10 and 12-20, based on their dependency from Claims 1 and 11, respectively, are patentable over Willey, as well as referenced of record. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(e) rejections of Claims 1-20.

Regarding Claims 21 and 26, Claims 21 and 26 are amended to recite the following claim feature which is neither inherently nor expressly disclosed by Willey:

once the provided audio authentication initialization information is authenticated by the host device according to audio authentication initialization information stored by the host device for initial authentication of the detected wireless device, providing the host device with one or more of a device identification code and a device personal identification number of the wireless device as device identification information to enable subsequent authentication of the wireless device. (Emphasis added.)

Applicants respectfully submit that the above described authentication of the wireless device based on audio authentication initialization information stored by the host device for initial authentication of the wireless device is analogous to amended Claims 1 and 11. Therefore, Applicants' argument provided above with regard to the §102(e) rejection of Claims 1 and 11 is equally applicable to the §102(e) rejection of Claims 21 and 26.

For at least the reasons provided above, the audio information disclosed by Willey refers to the play back or display of the digits of an antispoof variable for devices that are being paired by a user to perform a key agreement. As taught by Willey, the antispoof variable is generated to avoid man-in-the-middle attacks (see ¶ P. 5, ¶ 0048, lines 1-11.) As further disclosed by Willey, once the user gives a positive confirmation to, for example, the headset 300 and handset 100 that the digits of the antispoof variable are identical, the devices securely establish a link key which is used for BLUETOOTH authentication and encryption. (See pp. 5, ¶ 0048, lines 1-11.)

Conversely, as recited by amended Claims 21 and 26, a wireless device provides audio authentication initialization information to a host device which is authenticated by the host device according to audio authentication initialization information stored by the host device for initial authentication of the wireless device. For at least the reasons indicated above, the play back of the digits of the antispoof variable for verification by a user to enable establishment of a link key as part of a key agreement to provide BLUETOOTH authentication and encryption, as disclosed by Willey, neither expressly nor inherently discloses authentication by a host device using audio authentication initialization information stored by the host device for initial authentication of a wireless device, as recited by amended Claims 21 and 26.

Therefore, Applicants respectfully submit that amended Claims 21 and 26, as well as dependent Claims 22-25 and 27-30, based on their dependency from Claims 21 and 26,

respectively, are patentable over Willey, as well as referenced of record. Id. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(e) rejections of Claims 21-30.

Regarding Claim 31, Claim 31 is amended to recite the following claim feature which is neither expressly of inherently disclosed by Willey:

> an authentication unit to authenticate at least one wireless device detected within communications range of the apparatus using stored audio authentication initialization information for initial authentication of the wireless device if a challenge and response scheme for authentication according to device identification information of the detected wireless device fails to authenticate the detected wireless device. (Emphasis added.)

Applicants respectfully submit that the authentication of the detected wireless device using stored audio authentication initialization information is analogous to the previously recited features of amended Claims 1, 11, 21 and 26. Therefore, Applicants argument provided above with regard the §102(e) rejection of Claims 1, 11, 21 and 26 equally applied to the §102(e) rejection of Claim 31 as anticipated by Willey.

For at least the reasons indicated above, the audio play back of an antispoof variable to a user for completion of initial pairing of wireless devices to establish a link key for BLUETOOTH authentication and encryption, as though by Willey (see supra,) does not either expressly or inherently disclose the authentication of a detected wireless device using stored audio authentication initialization information for initial authentication of the detected wireless device if a challenge and response scheme for authentication according to device identification information of the detected wireless device fails to authenticate the detected wireless device, as recited by amended Claim 31.

Therefore, Applicants respectfully submit that amended Claim 31, as well as dependent Claims 32 and 33, are patentable over Willey, as well as referenced of record. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(e) rejections of Claims 31-33.

Regarding Claim 34, Claim 34, as amended, recites the following claim feature which is neither expressly of inherently disclosed by Willey:

> once provided the audio authentication initialization information is authenticated by the host device according to audio authentication initialization information stored by the host device for initial authentication of the detected wireless device, providing the host device with one or more of a device identification code and a device personal identification number of the wireless device as device identification information to enable subsequent authentication of the wireless device. (Emphasis added.)

Applicants respectfully submit that the above recited feature of amended Claims 34 is analogous to the previously recited feature of amended Claims 21 and 26. Therefore, Applicants argument provided above with regard the §102(e) rejection of Claims 21 and 26 equally applied to the §102(e) rejection of Claim 34 as anticipated by Willey.

Therefore, for at least the reasons indicated above, Applicants respectfully submit that the audio play back of the digits of an antispoof variable for verification by a user to enable completion of a key agreement for establishment of a link key for BLUETOOTH authentication and encryption, as taught by Willey (see supra,) fails to expressly or inherently disclose the authentication of a detected wireless device using audio authentication initialization information stored by a host device for initial authentication of the detected wireless device, as recited by amended Claim 34.

Consequently, for at least the reasons provided above, Applicants respectfully submit that amended Claim 34, as well as dependent Claims 35 and 36, are patentable over Willey, as well as referenced of record. Therefore, Applicants respectfully request that the Examiner reconsider and withdraw the §102(e) rejections of Claims 34-36.

CONCLUSION

In view of the foregoing, it is submitted that Claims 1-36, as amended, patentably define the subject invention over the cited references of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes a telephone conference would be useful in moving the case forward, he is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: December 14, 2006

By: _____
Joseph Lutz, Reg. No. 43,765

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING:
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail on the date shown below, with sufficient postage on the date below, in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Annie McNally — 12/14/06
Annie McNally — Date